

常问问题 • 08/2014

在 TIA 中组态安全模块 CPx43-1 Advanced 防火墙功能保护自动化单元

工业安全，防火墙，CP343-1，CP443-1

目录

1. 问题	3
1.1 介绍	3
1.2 概述	3
2. 自动化解方案	4
2.1 网络拓扑结构.....	4
2.2 硬件与软件需求	4
2.3 CP x43-1 Advanced V3	5
3. CP343-1 Advanced V3 防火墙功能的组态配置	6
3.1 配置概述	6
3.2 分配 IP 地址.....	7
3.3 创建 PLC 项目	9
3.4 启用 CP343-1 Advanced V3 安全功能	12
3.5 配置防火墙规则	13
3.6 下载组态到站点	14
3.7 测试防火墙功能	15

1. 问题

1.1 介绍

网络安全在工业自动化中变得越来越重要。在过去，自动化网络由于专有的现场总线从而成为物理上成为一个孤岛。随着以太网优势凸显使得在工业领域出现了大量基于以太网的解决方案。其具体体现为两个方面：一方面是工业生产越来越多的和以前民用化的网络相连接越来越紧密，以及通过办公网络需要采集获得生产网络的信息，与生产网络需要大量的信息的交换。另一方面现代的一些技术越来越多的应用到工业控制领域。两种体系的融合度越来越高。由于这方面的进展，工业通信面临着威胁，如从办公室或 IT 环境中的黑客、病毒、蠕虫和木马等。

1.2 概述

出于企业管理的要求，需要将自动化单元连接到公司内部网络，但仅允许网络中指定的设备或指定的通信服务访问自动化单元，如图 1 所示。

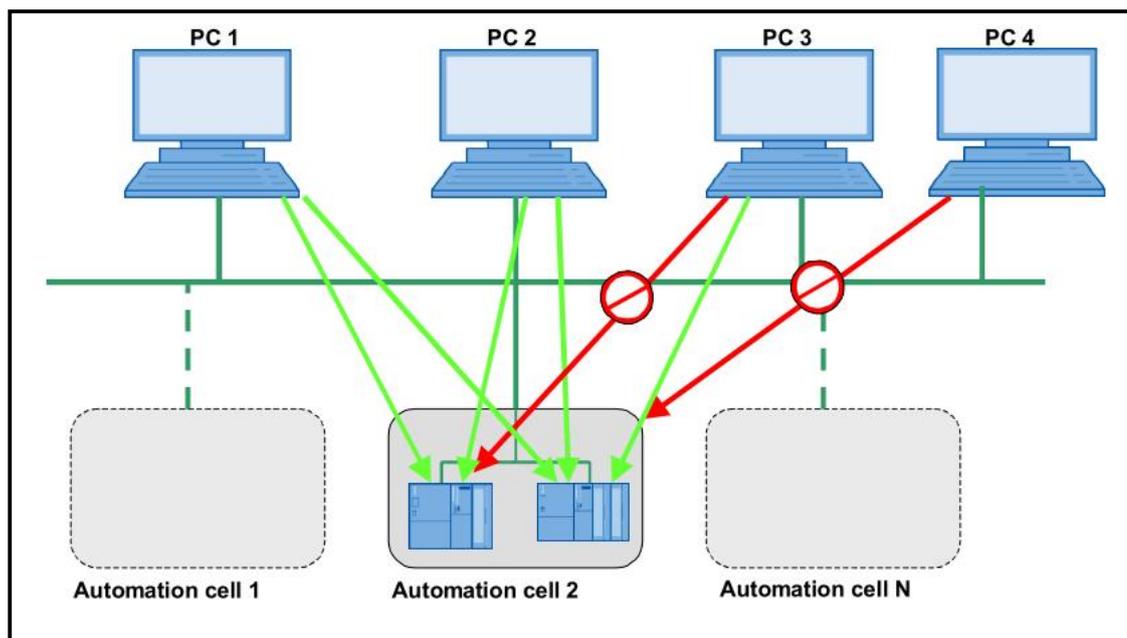


图 1 自动化需求

2. 自动化解决方案

2.1 网络拓扑结构

如图2所示，PC1（192.168.1.100/24）是工程师站；PC2（192.168.1.101）是普通的办公计算机。PLC通过CP343-1 Advanced V3的X1接口（外网口）连接到了办公网络。

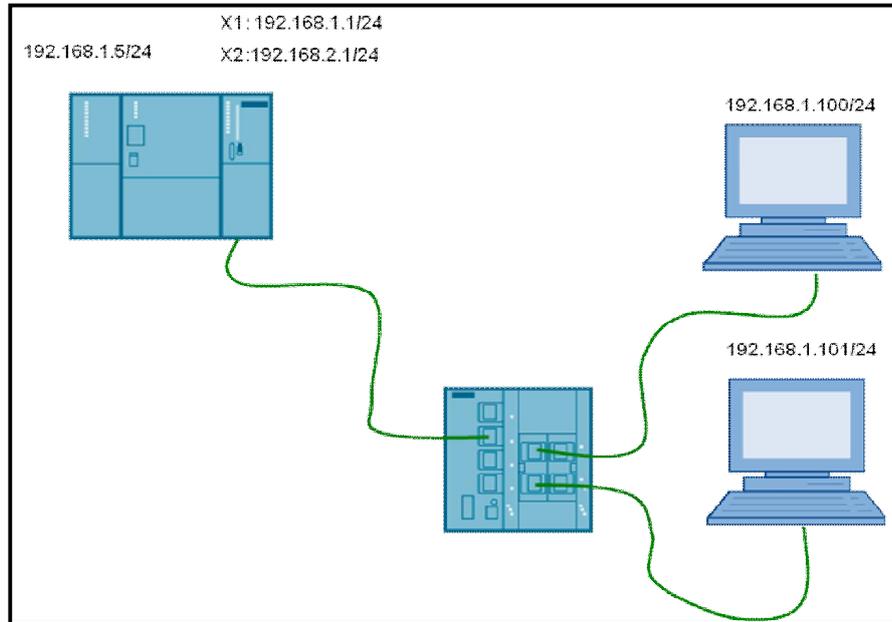


图 2 网络拓扑结构

2.2 硬件与软件需求

设备	数量	订货号	注释
电源 PS307 2A	1	6ES7 307-1BA00-0AA0	
CPU 317-2PN/DP	1	6ES7 317-2EK14-0AB0	可以使用任何其它与 CP343-1 AD 兼容的 CPU
CP 343-1 Advanced	1	6GK7 343-1GX31-0XE0	
SCALANCE X308-2M	1	6GK5 308-2GG00-2AA2	可以使用任何其它交换机
PC	2		

表 1 硬件列表

设备	数量	订货号	注释
STEP 7 Professional v13	2	6ES7822-1AA03-0YA5	
Windows 7 Ultimate SP1 64-bit Operating System	2		

表 2 软件环境

2.3 CP x43-1 Advanced V3

CP x43-1 Advanced V3 集成有防火墙功能。是西门子针对工业自动化工程安全理念的的实现的一部分。可以被配置为防火墙功能保护自动化单元。通过它很容易实现对自动化单元的保护，仅允许指定的设备访问自动化单元。



图 3 带安全功能的 CPx43-1 Advanced V3



提示!

CPx43-1 Advanced V3 的以太网的安全接口 X1 与 非安全接口 X2 对报文的处理是不同的。连接设备时这些端口不能混用。否则达不到保护功能!

3. CP343-1 Advanced V3 防火墙功能的组态配置

3.1 配置概述

网络拓扑如下图 4

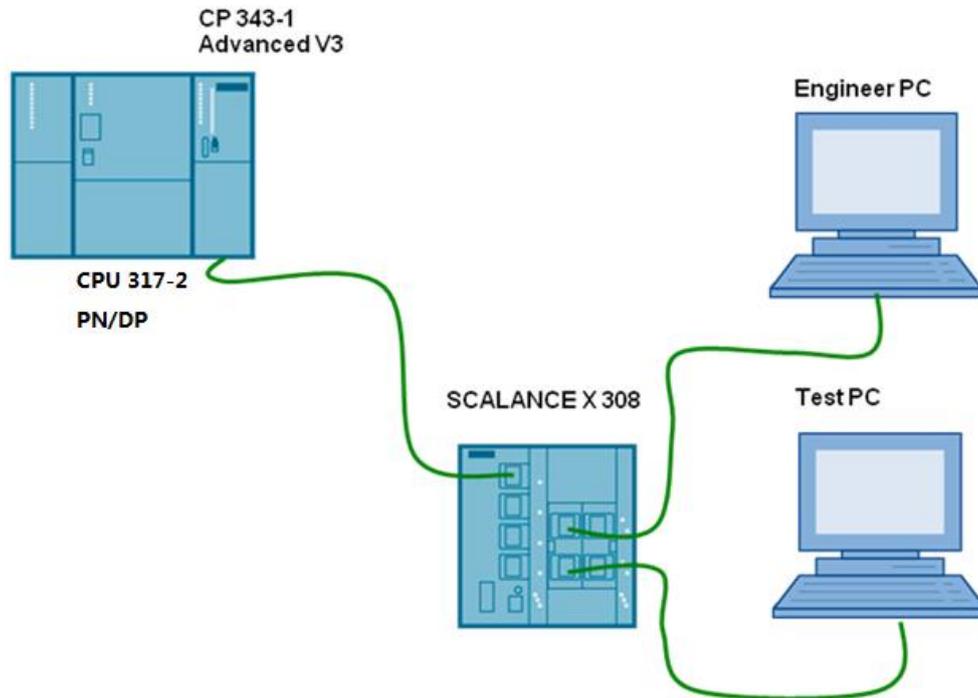


图 4 网络拓扑

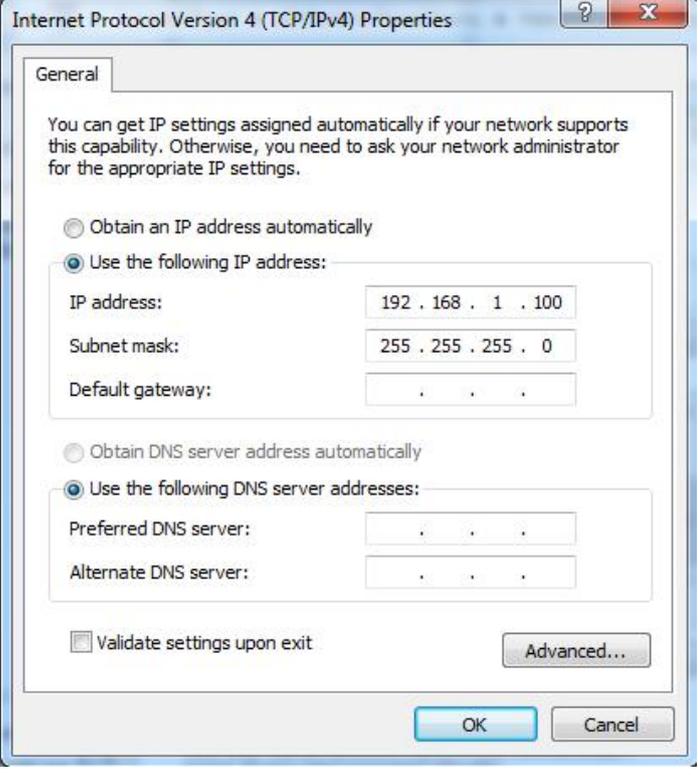
各设备的 IP 地址分配见表 3

	模块	IP 地址
外部网络	Engineer PC	192.168.1.100/24
	Test PC	192.168.1.101/24
内部网络	CPU 317 - 2PN/DP	192.168.0.1/24
	CP 343-1 Advanced V3 X1	192.168.1.1/24
	CP 343-1 Advanced V3 X2	192.168.2.1/24

表 3 IP 地址表

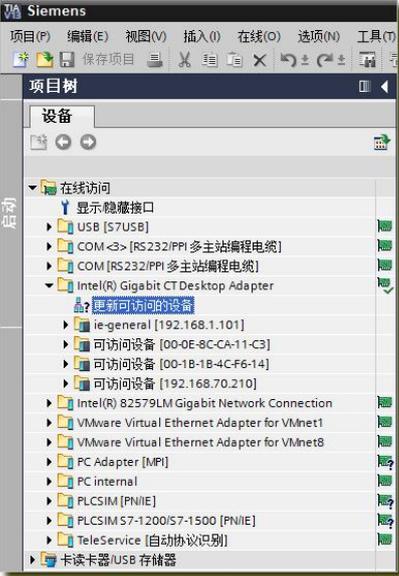
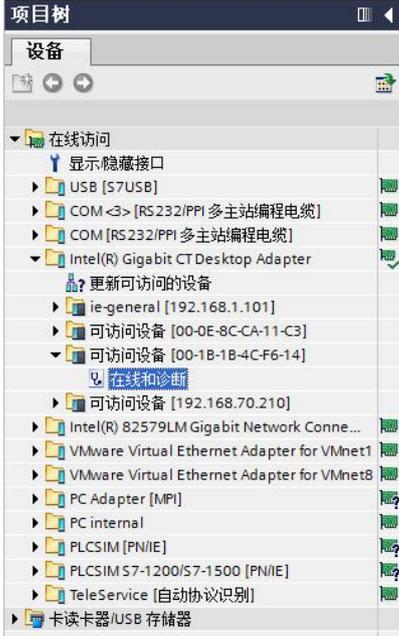
3.2 分配 IP 地址

根据IP 地址列表，通过如下的步骤配置 Engineer PC 和 Test PC 的 IP地址

步骤	操作	备注
1.	<p>选择 “开始 > 控制面板 > 网络和共享 > 本地连接 > 属性” 打开 Internet Protocol Version 4(TCP/IPv4). 按表 3 修改 Engineer PC 和 Test PC 的 IP 地址.</p> <p>注意: 对于路由模式，除此之外还需要输入网关地址。</p>	

分配模块的IP地址

为了下载 STEP 7 项目到 CPU。需要修改 CPU 或 CP卡的 IP 地址。

步骤	操作	备注
1.	连接 Engineer PC 到 SCALANCE X308 的其中一个端口上，然后连接 CP343-1 的X1接口到SCALANCE X308 的另一个端口。	连接两个设备到同一个以太网物理网上
2.	在 Engineer PC 上打开 TIA v13。进入项目视图，展开项目树下“在线访问”，选择实际使用的物理网卡，双击“更新可访问节点的设备”	
3.	按照打印在CP343-1模块上的X1接口MAC地址确定需要分配IP地址的设备，本案例为00-1B-1B-4C-F6-14，展开“可访问设备 [00-1B-1B-4C-F6-14]”，双击“在线和诊断”	

步骤	操作	备注
4.	在工作区选择“功能”下的“分配IP地址”，输入IP地址192.168.0.1和子网掩码255.255.255.0，点击“分配IP地址”，操作成功后可在巡视窗口信息页面看见“参数已成功传送”消息	

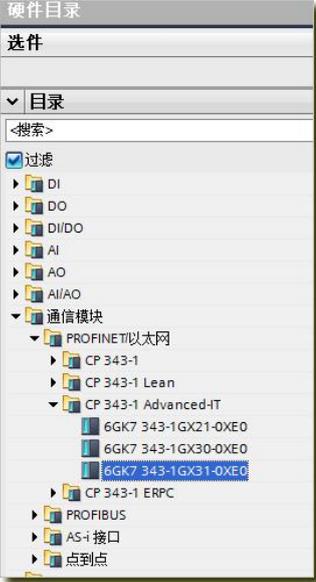
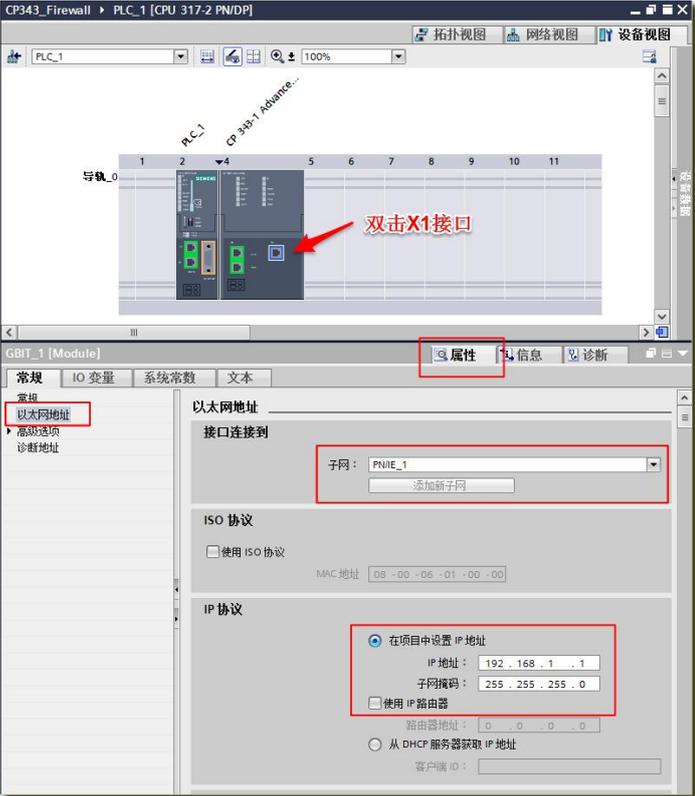
注意：对于已开启安全功能的 CP343-1 Advanced V3，可能无法进行以上操作，可先设置 CPU 集成 PN 口的 IP 地址，通过 CPU PN 接口下载硬件组态，使 CP343-1 新的安全功能生效。

3.3 创建 PLC 项目

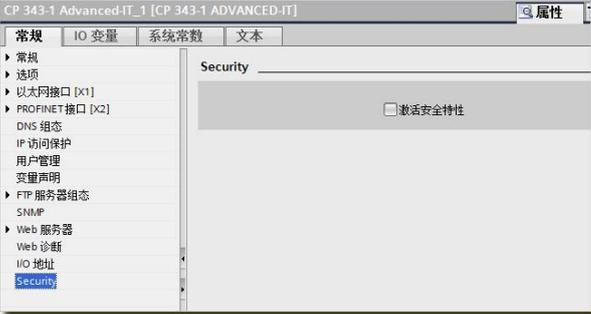
在 STEP里创建一个项目并插入CPU317-2PN/DP 站。操作步骤如表6

步骤	操作	备注
1.	在 Engineer PC 上打开 TIA v13。在“项目”菜单中选择“新建...”选项	
2.	在弹出的创建新项目窗口里输入项目名称为“CP343_Firewall” 点击“创建”按钮	

步骤	操作	备注
3.	在项目树 CP343_Firewall 下点击“添加新设备”	 <p>The screenshot shows the Siemens CP343_Firewall project tree. The 'Add New Device' button is highlighted in blue. The tree structure includes: 设备 (Devices), CP343_Firewall, 添加新设备 (Add New Device), 设备和网络 (Devices and Networks), 公共数据 (Public Data), 文档设置 (Document Settings), 语言和资源 (Languages and Resources), 在线访问 (Online Access), and 卡读卡器/USB 存储器 (Card Reader/USB Storage).</p>
4.	输入设备名称 PLC_1, 选择控制器, SIMATIC S7-300 下的 CPU317-2PN/DP, 选择实际使用 CPU 的订货号以及版本号, 本案例使用的是 6ES7317-2EK14-OAB0 V3.2, 点击“确认”后进入设备视图	 <p>The screenshot shows the 'Add New Device' dialog box. The device name is 'PLC_1'. The 'Controller' category is selected. Under 'SIMATIC S7-300', the 'CPU 317-2 PN/DP' is selected. The order number is '6ES7 317-2EK14-OAB0' and the version is 'V3.2'. The 'Open Device View' checkbox is checked. The 'OK' button is highlighted.</p>

步骤	操作	备注
5.	在硬件目录中选择实际使用的CP343-1 Advanced模块，双击模块，CP343-1将添加至CPU机架中	 <p>The screenshot shows a software interface for selecting hardware modules. Under the '目录' (Catalog) section, the '通信模块' (Communication Modules) folder is expanded to show 'PROFINET 以太网' (PROFINET Ethernet). Within this, 'CP 343-1 Advanced-IT' is selected, and the specific model '6GK7 343-1GX31-0XE0' is highlighted.</p>
6.	<p>在工作区设备视图下双击CP343-1 X1接口，巡视窗口下属性页，“常规”中选择“以太网地址”，为X1接口添加子网PN/IE_1, 设置IP地址192. 168. 1. 1和子网掩码255. 255. 255. 0 ；</p> <p>类似操作为CP343-1 X2接口添加子网PN/IE_2, 设置IP地址192. 168. 2. 1和子网掩码255. 255. 255. 0</p> <p>CPU PN接口添加子网PN/IE_3, 设置IP地址192. 168. 0. 1和子网掩码255. 255. 255. 0</p>	 <p>The screenshot shows the configuration window for the '以太网地址' (Ethernet Address) of the CP 343-1 X1 interface. A red arrow points to the 'X1' port in the device view above. In the configuration window, the '子网' (Subnet) is set to 'PN/IE_1'. Under the 'IP 协议' (IP Protocol) section, the option '在项目中设置 IP 地址' (Set IP address in project) is selected, with the IP address set to '192.168.1.1' and the subnet mask to '255.255.255.0'.</p>

3.4 启用 CP343-1 Advanced V3 安全功能

步骤	操作	备注
1.	在工作区设备视图下点击CP343-1，巡视窗口下属性页面“常规”中选择“Security”，点击“用户登录”按钮	
2.	输入 用户名：admin234 密码：admin234 点击“登录”按钮	
3.	项目树中新增“全局安全设置”条目，右侧出现的开锁图标表示用户登录成功，可以进行安全设置	
4	返回设备视图下CP343-1属性，此时Security已经允许进行设置，勾选“激活安全特性”	



3.5 配置防火墙规则

在本应用案例中只允许 IP地址为192.168.1.100的Engineer PC的S7协议数据通过防火墙，不允许其他任何计算机的任何协议通过防火墙访问内网的节点。

在IP规则列表双击动作列“新增”，选择Allow，“来自”列选择“外部”，“至”选择“站”，源IP地址输入“192.168.1.100”，“服务”列中选择预定义的服务“S7”，如图5，此规则表示允许来自IP地址为192.168.1.100外部网络设备对CP343-1的S7服务访问，对于其他未明确定义允许通过的数据包都被防火墙过滤掉。

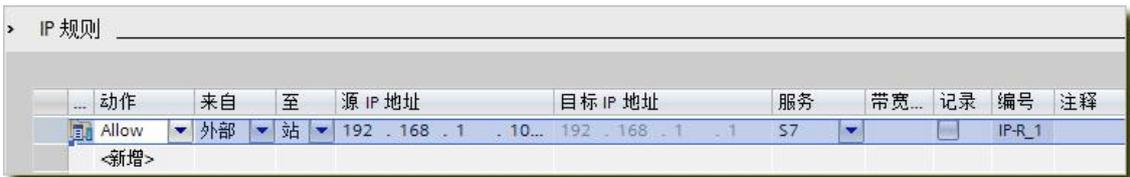


图 5 防火墙规则

3.6 下载组态到站点

如图6在项目树中点击PLC_1，点击工具栏中的下载图标，弹出下载对话框如图7所示。

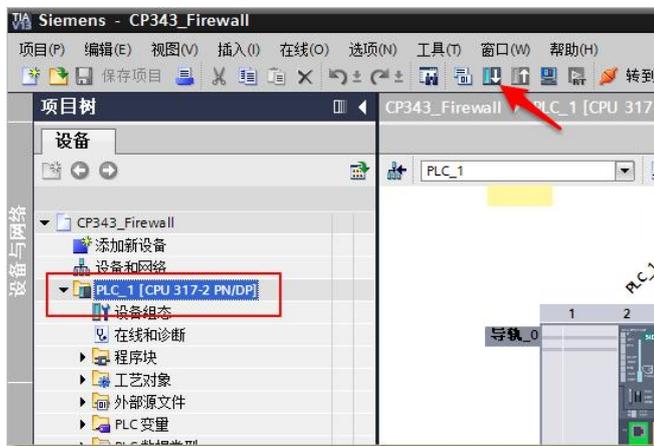


图 6 下载站点配置

下载对话框设置

- PG/PC 接口的类型下拉框中选择 PN/IE
- PG/PC 接口下拉框中选择连接 CP343-1 的实际以太网卡
- 接口/子网的连接下拉框选择 CP343-1 连接的子网 PN/IE_1
- 点击“开始搜索”按钮，搜索网络连接的兼容设备
- 在兼容设备列表中选择搜索出的设备 CP343-1 Ad
- 点击“下载”按钮，按照提示完成站点下载

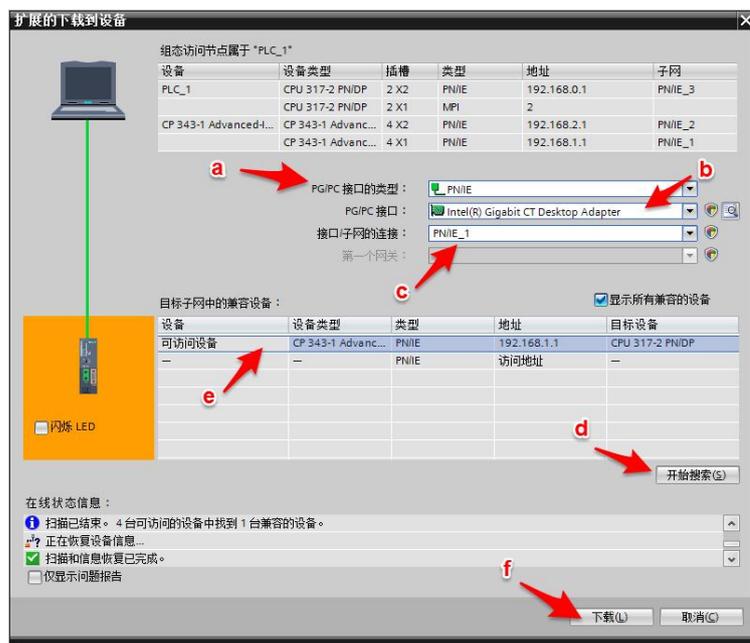


图 7 下载对话框

3.7 测试防火墙功能

下载后，连接 Test PC 到 SCALANCE X308 上。通过 Test PC 下载硬件配置到 CPU 时，此通信被 CP343-1 防火墙阻止。通过 Engineer PC 下载硬件配置到 CPU 时，通信是被允许。